PCT/DE 00/01544 Kopie für Anmelder

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G06K 19/073

A1

(11) Internationale Veröffentlichungsnummer: WO 98/18102

(43) Internationales Veröffentlichungsdatum: 30. April 1998 (30.04.98)

(21) Internationales Aktenzeichen: PCT/AT97/00225

(22) Internationales Anmeldedatum: 20. Oktober 1997 (20.10.97)

(30) Prioritätsdaten:
A 1858/96 22. Oktober 1996 (22.10.96) AT

(71)(72) Anmelder und Erfinder: POSCH, Reinhard [AT/AT]; Klosterwiesgasse 32/1, A-8010 Graz (AT).

(74) Anwälte: BRAUNEISS, Leo usw.; Landstrasser Hauptstrasse 50, A-1030 Wien (AT).

(81) Bestimmungsstaaten: AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO Patent (GH, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

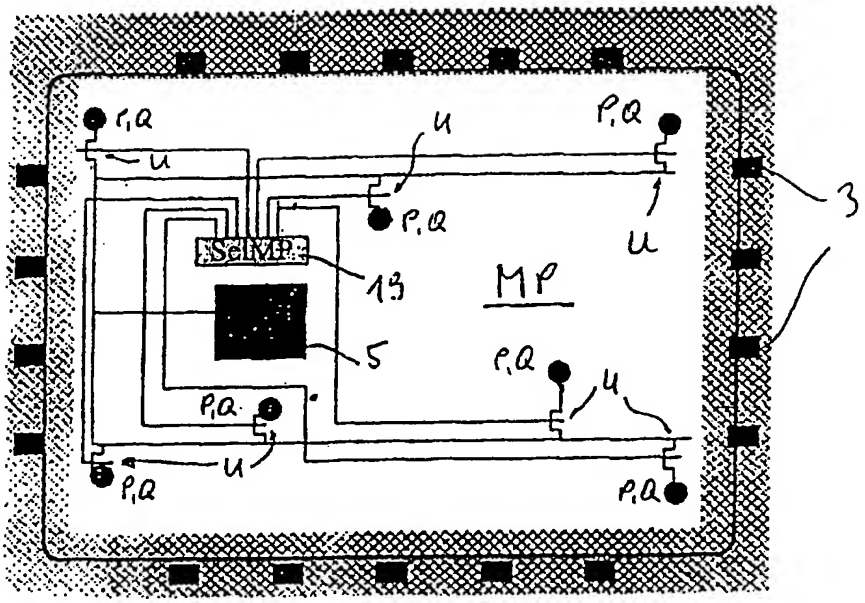
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD AND ARRANGEMENT FOR PROTECTING ELECTRONIC COMPUTING UNITS, IN PARTICULAR CHIP CARDS

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUM SCHUTZ VON ELEKTRONISCHEN RECHENEINHEITEN, INSBESONDERE VON CHIPKARTEN

(57) Abstract

The invention concerns a method and arrangement for protecting electronic computing units from undesired access. According to the invention, the side of the unit (1) exposed to attack is provided with a casing (2) having inhomogeneous properties. The unit (1) determines measured values at at least one set measuring point on the casing (2) when specific signals have been applied by the unit (1) to the casing (2) at a set signal-output point, a signature characteristic of an intact casing (2) at the time of the measurement being formed using the measured values.



(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren und eine Anordnung zum Schutz von elektronischen Recheneinheiten gegen unerwünschten Zugriff. Erfindungsgemäß ist vorgesehen, daß die einem Angriff ausgesetzte Seite der Einheit (1) mit einer Ummantelung (2) mit inhomogenen Eigenschaften versehen wird, daß von der Einheit (1) Meßwerte an zumindest einer festgelegten Meßstelle an der Ummantelung (2) ermittelt werden, nachdem an einer festgelegten Signalaufgabestelle an die Ummantelung (2) von der Einheit (1) definierte Signale angelegt wurden, und daß mit den Meßwerten eine für eine unversehrte Ummantelung (2) zum Zeitpunkt der Vermessung charakteristische Signatur gebildet wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren und Anordnung zum Schutz von elektronischen Recheneinheiten, insbesondere von Chipkarten.

Die Erfindung betrifft ein Verfahren gemäß dem Oberbegriff des Patentanspruches 1. Des weiteren betrifft die Erfindung eine Anordnung gemäß dem Oberbegriff des Patentanspruches 18.

Bekannt ist der Schutz von Daten und Programmen, die in elektronischen Einheiten bzw. Schaltungen enthalten sind, durch Verschlüsselung dieser Daten und Programme oder durch elektrische und/oder mechanische, den Zugriff bzw. den Zutritt verhindernde Schutzmaßnahmen, wie z.B. Codekarten für eine Zutrittsberechtigung bzw. die Anordnung derartiger Einheiten in Sicherheitsräumen usw.. Wird bei derartig gesicherten Einheiten der vorgesehene Schutz ausgeschaltet bzw. durchdrungen, so wird ein Ausspähen des gegebenenfalls verschlüsselt enthaltenen Inhalts der elektronischen Einheiten möglich. Als Beispiel wird dazu auf mit Codekarten gesicherte Türen von zutrittsgesicherten Rechenanlagen verwiesen. Bei einer Reihe von Recheneinheiten bzw. Datenträgern, z.B. Chips auf Chipkarten, erfolgt eine Sicherung gegen ein Ausspähen von Daten und Programmen lediglich durch Verschlüsselung dieser Daten; eine Sicherung gegen unerlaubten Zugriff zum Chip ist minimal oder nicht gegeben; bei einer Chipkarte ist ein mechanischer Zugriff auf die Daten bzw. deren Entnahme meist nach chemischer Entfernung der Kunststoffschicht mit einer durch eine vorhandene Passivierungsabdeckung des Chips durchgestochenen Tastnadel möglich.

Das wesentliche Ziel der Erfindung ist somit ein Schutz von elektronischen Einheiten gegen ein Ausspähen, insbesondere durch mechanische Manipulationen bzw. Angriffe jeglicher Art. Ein weiteres wesentliches Ziel der Erfindung ist es zu verhindern, daß selbst für den Fall, daß mechanisch Zutritt zu der elektronischen Einheit erlangt wird, ein Ausspähen bzw. Auslesen und ein Weiterverwenden von Daten und/oder Programmen, die in der elektronischen Einheit enthalten sind und/oder ein ordnungsgemäßer weiterer Betrieb dieser Einheit nach dem Zugriff unmöglich gemacht wird. Schließlich ist es weiteres Ziel der Erfindung, mit einer derart geschützten Einheit den Schutz von von dieser Einheit unabhängigen Gegenständen zu erreichen.

Diese Ziele werden bei einem Verfahren der eingangs genannten Art durch die im Kennzeichen des Anspruches 1 angeführten Merkmale erreicht. Bei einer Anordnung der eingangs genannten Art wird dieses Ziel durch die im Kennzeichen des Patentanspruches 18 angeführten Merkmale erreicht.

Grundlage für die erfindungsgemäße Vorgangsweise ist eine Feststellung der Unversehrtheit der bei einem unerwünschten Zugriff zu der zu schützenden elektronischen Einheit zu überwindenden Ummantelung. Jede Verletzung bzw. Beschädigung der

Ummantelung durch eine mechanische oder anders geartete Einwirkung beim Zugriff verändert unwiderruflich und unnachahmbar deren Eigenschaften, insbesondere deren elektrische Eigenschaften. Eine Verletzung der Ummantelung führt dazu, daß die Einheit nicht mehr ordnungsgemäß in Funktion gesetzt werden kann, weil die bei der Initialisierung der Einheit ermittelte Signatur zur Programmabarbeitung bzw. Entschlüsselung der ursprünglich gespeicherten Daten und/oder Programmen benötigt wird nicht zur Verfügung steht und nicht mehr erstellt werden kann oder weil die Einheit bei Feststellung einer sich gegenüber der ursprünglich ermittelten Signatur veränderten Signatur ihre Funktion einstellt. Die Einheit ist durch die Ummantelung geschützt bzw. befindet sich im Inneren der Ummantelung, und agiert von dieser geschützten Lage aus. Jeder Versuch, mechanisch Zutritt zur Einheit zu erhalten, ist zum Scheitern verurteilt, da jeder Zugriff eine mechanische Beschädigung der Ummantelung bewirkt, sei es z.B. durch Anbringung von Öffnungen oder Versuche, die Schutzschicht zu penetrieren, wodurch es zu einer bleibenden Veränderung ihrer Eigenschaften und somit der Signatur kommt. Bei Anordnung einer entsprechenden Zahl von Signalaufgabestellen und Meßpunkten, z.B. in dem Ausmaß von jeweils vier Stellen bzw. Punkten je cm^2, wird es bereits mit geringem Meßaufwand gut möglich, durch Nadelstiche auf dieser Fläche von 1 cm^2 hervorgerufene Eigenschaftsänderungen der Ummantelung festzustellen.

Aufgrund der erfindungsgemäßen Vorgangsweise erhält ein Eingreifer durch Manipulationen auf technisch-physikalischer Ebene, insbesondere durch mechanischen Angriff keine relevanten Informationen bezüglich der Daten und/oder Programme, die in der Einheit unter Verwendung der Signatur gespeichert vorliegen oder abgearbeitet werden; dies insbesondere deshalb, da die bei der Initialisierung eingespeicherten Daten und/oder Programme mit der Signatur verschlüsselt sind, diese Signatur aber vorteilhafterweise nicht abgespeichert wird. Somit ist bei jeder Inbetriebnahme die Signatur neu zu ermitteln, was erfolgreich nur möglich ist, solange die Ummantelung bezüglich ihrer vermessenen Eigenschaften invariant verbleibt. Besonders vorteilhaft ist eine derartige Vorgangsweise für den Schutz von Chips, insbesondere VLSI-Chips, wie sie in Chipkarten enthalten sind.

Prinzipiell ist es möglich, Mikroprozessoren, Recheneinheiten, Platinen oder auch beliebig große, diese Einheiten enthaltende Einrichtungen mit derartigen Schutzschichten bzw. Ummantelungen, gegebenenfalls auf Teilbereichen oder über ihre gesamten Oberflächen zu versehen. Die geschützten Einheiten stehen lediglich über die zum Datentransfer vorgesehenen Übertragungseinheiten, z.B. Leitungen, Antennen, Sender für Magnetimpulse oder elektrische Impulse, Datenleitungen usw. mit externen elektronischen Einrichtungen in Verbindung. Zur Ermittlung der Signatur bzw. zur Feststellung der Unversehrtheit der Ummantelung oder zur Überprüfung der Signatur bzw. zur gewünschten Verwendung der Signatur während des Betriebs der Einheit, sind in der Einheit

entsprechende Daten und/oder Programme a priori gespeichert enthalten bzw. bei der Initialisierung zumeist mit der Signatur verschlüsselt eingespeichert worden, die eine entsprechende Funktion der Einheit gewährleisten, jedoch ohne von außen her bei dieser Tätigkeit beeinflußt werden können.

Das vorliegende Verfahren verhindert zwar nicht einen mechanischen bzw. gewaltsamen Zutritt bzw. Zugriff zu den elektronischen Einheiten oder ein Abfühlen des Inhaltes dieser Einheiten, jedoch wird das Gewinnen von "brauchbaren" Informationen bei der Attacke gänzlich verhindert; das Resultat dieser die Signatur selbst unwiderruflich abändernden Attacke ist es, daß aufgrund der geänderten Signatur bzw. nicht mehr ordnungsgemäß erfolgenden Entschlüsselung der gespeicherten Daten und/oder Programme ein Fehlverhalten der Einheit eintritt und diese Einheit somit völlig unbrauchbar geworden ist.

Die Signatur der Ummantelung ist nicht nachbildbar, da die bei der Initialisierung ermittelte ursprüngliche Signatur nicht bekannt und vorteilhafterweise auch nicht gespeichert ist und auch die bei einer Verletzung der Ummantelung hervorgerufenen Änderungen der Signatur nicht erkannt werden können. Des weiteren können die dem initialen Ermittlungsverfahren für die Signatur zugrundeliegenden Daten und Parameter der Einheit nicht ausgelesen werden, da programmäßig Vorkehrungen gegen ein derartiges Auslesen vorgesehen werden können und ferner eine Entschlüsselung der gespeicherten Daten nur bei Kenntnis der ursprünglichen, bei der Attacke aber veränderten, Signatur in richtiger Weise erfolgen könnte. Für den Fall aber, daß die Signatur durch einen mechanischen Eingriff in nicht behebbarer und nicht nachahmbarer Weise abgeändert worden ist, sind allerdings die gespeicherten Daten und Programme unwiderruflich verloren. Es ist zwar möglich, die Einheit, soferne sie durch den Zugriff nicht Schaden erlitten hat, als Bauteil weiter zu verwenden bzw. neu zu initialisieren bzw. zu programmieren; die in ihr enthaltene Funktion bzw. enthaltenen Daten sind jedoch unwiderruflich verloren.

Unter Signatur wird jede unter Verwendung von bei unverletzter Ummantelung invariant bleibenden Größen bzw. Meßwerten ermittelte Wertezusammenfassung verstanden; diese Zahl wird mit einer vorgegebenen Stellenanzahl bzw. auf diese Stellenanzahl gerundet festgelegt.

Vorteilhafte Ausführungsformen der Erfindung sind der folgenden Beschreibung, den Zeichnungen und den Patentansprüchen zu entnehmen.

Im folgenden wird die Erfindung anhand der Zeichnungen näher erläutert.

Fig. 1 zeigt das Prinzip einer erfindungsgemäß gesicherten Einheit, Fig. 2 und 3 zeigen schematisch eine Draufsicht und einen Schnitt durch eine erfindungsgemäße Einheit. Fig. 4 zeigt schematisch den Schaltungsaufbau einer erfindungsgemäßen Einheit und Fig. 5, 6, 7 und 8 schematisch Anwendungsbeispiele.

Fig. 1 zeigt schematisch eine erfindungsgemäß geschützte Einheit 1, im vorliegenden Fall einen Modul bzw. eine mit Hardware bestückte Platine, der bzw. die von einer Schutzschicht bzw. Ummantelung 2 allseitig umgeben ist. Diese Ummantelung 2 kann eine die Einheit 1 ein-, mehr- oder allseitig umgebende (Kunststoff)Schicht sein, die vorteilhafterweise zumindest längs einer Dimension bezüglich ihrer elektrischen und/oder elektromagnetischen Eigenschaften inhomogen ist. Eine derartige Inhomogenität kann z.B. durch Änderungen der Dicke der (Kunststoff)Schicht und/oder durch Einschluß von nicht bzw. nicht leicht mit dem Schichtmaterial z.B. Glas, Polymeren bzw. Kunststoff, Gummi, Metall- bzw. Halbmetallfilmen, Papier od.dgl. mischbaren, unregelmäßig verteilten Materialien bewirkt werden, insbesondere, wenn diese Materialien z.B. Metallpigmente, Metallfäden, Rußpartikel, Kohlefasern od.dgl. sind. Bei der Wahl dieser Materialien sollte auch darauf Rücksicht genommen werden, daß im Falle einer mechanischen Beschädigung relativ große Änderungen der Eigenschaften der Ummantelung bewirkt werden, sodaß Änderungen in der durch diese geänderten Materialeigenschaften bedingten Werte der Signatur entsprechend groß und leicht feststellbar sind. Vorteilhafterweise liegt die elektrische Leitfähigkeit der Ummantelung zwischen der eines Isolators und der eines metallischen Leiters, um die Empfindlichkeit der Meßsensoren und die Anzahl der Stellen P, Q in Grenzen halten zu können. Die Dicke der Ummantelung 2 ist nicht von grundsätzlicher Bedeutung und hängt vom Anwendungsfall ab.

Als zu schützende Einheiten 1 kommen insbesondere Prozessoren, Recheneinheiten, Chips, Mikroprozessoren bzw. alle elektronischen Bauteile bzw. Konfigurationen in Frage, die selbsttätig Rechenoperationen bzw. selbständig die vorgegebenen Schritte zur insbesondere initialen Ermittlung einer Signatur bewältigen bzw. ein entsprechendes Programm abarbeiten können bzw. alle Einrichtungen und Gegenstände, die derartige Einheiten 1 umfassen.

In Fig. 2 ist schematisch als zu schützende Einheit 1 ein nicht im Detail dargestellter Mikroprozessor MP gezeigt, der Anschlüsse 3 besitzt, die aus der Ummantelung 2 herausgeführt sind. Wie Fig. 3 im Schnitt zeigt, ist in diesem Fall der Mikroprozessor MP nur auf seiner Oberfläche von der Ummantelung 2 abgedeckt. Die Mikropads bzw. Anschlüsse 3 können auf übliche Weise mit einer Abdeckschicht 6 gegen elektrischen Kontakt mit der Ummantelung 2 abgedeckt sein und die Ummantelung 2 schützt den Mikroprozessor MP gegen einen mechanischen Angriff auf seiner diesbezüglich empfindlichen Oberfläche. Ein Angriff gegen den Mikroprozessor MP auf dessen Unter- bzw. Trägerseite 4 würde diesen bereits durch den stattfindenden Angriff selbst zerstören.

Um entsprechende Verbindungen zwischen der zu schützenden Einheit 1 und der Ummantelung 2 für die Signalbeaufschlagung in Signalaufgabestellen P und für die Messung der Meßwerte in Meßstellen Q zu erstellen, kann insbesondere bei Chips oder Mikroprozessoren die oberste Aufbauschichte 18 dieser Einheiten (Fig. 5) selbst

herangezogen werden oder es werden entsprechende elektrische Leiter(bahnen) 14, insbesondere in der obersten Struktur eines Mikroprozessors MP, verwendet bzw. ausgebildet, die an den Signalaufgabestellen P und Meßstellen Q mit der Ummantelung 2 in Verbindung stehen. Es ist insbesondere bei Chipkarten vorteilhaft, wenn diese Stellen sehr klein, in der Größenordnung von einigen μm^2, ausgebildet werden; bei Platinenummantelungen sind Stellen mit Flächen im mm^2-Bereich durchaus möglich. Zur Ausbildung der Signalaufbringungsstellen P und der Meßstellen Q können die Leiterbahnen 14 bis auf kleine leitende Bereiche mit einer elektrisch isolierenden Schicht abgedeckt werden und diese Bereiche stehen mit der Ummantelung 2 kontaktmäßig in Verbindung.

An Signalaufgabestellen P werden von der Einheit 1 selbst Signale, insbesondere elektrische Signale bzw. Signalimpulse, z.B. Strom und/oder Spannungswerte und/oder elektromagnetische Signale (Felder), beliebiger Art angelegt. Diese Signale werden vom Mikroprozessor MP bzw. von der Einheit 1 selbst bzw. von von der Einheit gesteuerten Signalgeneratoren gemäß den bei der Initialisierung unabänderlich vorgegebenen Daten und/oder Programmen erzeugt und gegebenenfalls über eine Verteileinrichtung, z.B. einen Selektor 19 oder einen Buffer 11 an zumindest eine, vorzugsweise eine Anzahl von Signalaufgabestelle(n) P angelegt. Ein oder eine Mehrzahl dieser Signal(e) wird (werden) mit definierter Größe und/oder Zeitdauer gleichzeitig oder in vorgegebener zeitlicher Reihenfolge an die festgelegten Signalaufgabestellen P angelegt.

In den Meßstellen Q werden mit Sensoren, z. B. elektromagnetischen Meßeinheiten bzw. Analog/Digitalwandler 5, die von der Signalbeaufschlagung resultierenden Meßgrößen abgenommen. Die Ermittlung bzw. Abnahme der Meßwerte erfolgt gleichzeitig oder zeitverzögert zu der Signalaufbringung für eine definierte Zeitspanne und/oder zu definierten Zeitpunkten, gegebenenfalls gleichzeitig für mehrere Meßstellen Q. Es ist auch möglich, eine statische Signalaufbringung und eine statische Messung vorzunehmen.

Prinzipiell ist es auch möglich, an einer Signalaufgabestelle P mehrere Signale hintereinander aufzugeben. Vorteilhafterweise wird jedoch derart vorgegangen, daß in einer unveränderlich vorgegebenen Mehrzahl von lagemäßig invarianten Signalaufgabestellen P unveränderlich definierte, insbesondere für die einzelnen Signalaufgabestellen unterschiedliche Signale an die Ummantelung 2 angelegt werden und daß an einer unveränderlich vorgegebenen Mehrzahl von lagemäßig invarianten Meßstellen Q die resultierenden Meßwerte in vorgegebener Weise abgenommen werden. Die Aufgabe der Signale und die Ermittlung der Meßwerte erfolgt immer nach denselben invarianten Kriterien, sodaß bei jedem Signalaufgabe-Meßwertermittlungs-Zyklus dieselben Resultate zu erwarten sind. Diese Resultate bleiben invariant, solange die Ummantelung 2 unveränderten Aufbau bzw. unveränderte Eigenschaften besitzt und sind für die Schutzschicht bzw. Ummantelung 2 und somit auch für geschützte Einheit 1 charakteristisch. Sobald eine Veränderung der Signatur der Ummantelung 2 durch

mechanische oder eine andere Veränderung, z. B. Durchbohren oder Anritzen, ihres Aufbaus eintritt, geht die bei der Initialisierung ermittelte und seit diesem Zeitpunkt invariant gültige Signatur unwiderruflich verloren und da eine geänderte Signatur von der Einheit für die Entschlüsselung der gespeicherten Daten und/oder Programme bzw. für ihren Betrieb nicht verwendet werden kann, ist ein sinnvoller Betrieb dieser Einheit nicht mehr möglich.

Die erhaltenen Meßwerte können entweder in der erhaltenen Form zu einer Signatur zusammengefaßt werden oder sie werden zur Signaturermittlung mittels vorgegebener Funktionen mathematisch miteinander verknüpft, z.B. kann ein Zahlenvektor der Meßwerte als Signatur für die Ummantelung bestimmt werden. Die Signatur könnte auch von der Zahl gebildet werden, die durch mathematische Abänderung der Meßwerte, z.B. Einsetzen der Meßwerte in Funktionen als Veränderliche ermittelt wird. Jede derart ermittelte Signatur bzw. Zahl bleibt invariant bzw. kann in derselben Form bzw. Größe immer wieder ermittelt werden, solange die Ummantelung 2 bezüglich ihrer Eigenschaften invariant bleibt. An sich können auch die von der Einheit 1 an die Ummantelung 2 abgegebenen Signale in der Signatur Berücksichtigung finden. Auch weitere invariante Daten könnten in der Signatur berücksichtigt werden; auch das Einsetzen der ermittelten Meßwerte in eine (HASH)-Funktion ist möglich; die sich ergebenden Funktionswerte können Teil der bzw. die Signatur sein. Die Ermittlung der Signatur erfolgt jedoch immer auf die bei der Initialisierung vorgegebene Weise.

Die dem Mikroprozessor bzw. Rechner für seine Funktion bzw. seinen Betrieb aufgegebenen Daten und/oder Programme werden bei der Initialisierung der Einheit 1 zumindest teilweise mit der initial ermittelten Signatur verschlüsselt gespeichert, sodaß bei jedem Betriebsbeginn diese Daten und/oder Programme sinnvollerweise nur dann abgearbeitet werden können, wenn für diese Abarbeitung - gegebenenfalls innerhalb vorbestimmter Grenzen - die zur Verschlüsselung eingesetzte Signatur bei der bei Betriebsbeginn jeweils neuerlich erfolgenden Signaturermittlung richtig erhalten wird. Es wird somit vor jeder neuen Betriebsaufnahme die Signatur neu ermittelt und entweder mit der initial ermittelten Signatur verglichen oder es wird vorgesehen, daß die unter Verwendung der initialen Signatur verschlüsselt gespeicherten Daten und/oder Programme zwangsläufig nur mit der neuen Signatur entschlüsselt bzw. abgearbeitet werden können. In beiden Fällen führt eine Diskrepanz zwischen der initialen und neu ermittelten Signatur zu einer Fehlfunktion der Einheit. Vorteilhafterweise wird die initial ermittelte Signatur nicht gespeichert, sondern wird gelöscht bzw. verworfen, nachdem sie zum Verschlüsseln der initial aufgegebenen Daten und/oder Programme verwendet wurde. Damit wird die Sicherheit gegen Zugriff bzw. Entschlüsselung des Inhaltes der Einheit erhöht.

Fig. 4 zeigt schematisch einen Aufbau eines mit ergänzenden elektronischen Bauteilen 5, 11 und Leitungen 14 versehenen Mikrochips, wobei von dem Prozessor MP über einen Buffer 11 elektrische Signale an die Signalaufgabestellen P abgegeben werden.

Der Empfang der Meßgrößen von den Meßstellen Q erfolgt übereinen Meßsensor 23 und den Analog/Digitalwandler 5. Es kann vorgesehen sein, daß sowohl der Buffer 11 als auch der Analog/Digitalwandler 5 einen Selektor umfassen, mit dem die Signale gleichzeitig und/oder der Reihe nach an eine Mehrzahl von Signalaufgabestellen P angelegt werden können bzw. eine Anzahl von Meßsensoren 23 bzw. Meßstellen Q gleichzeitig oder der Reihe nach abgetastet werden können. Die geschützte Einheit 1 kann über eine Datenaustauschleitung 9 mit einer externen Einheit 10 kommunizieren, ohne daß der Schutz für die elektronische Einheit 1 in irgendeiner Weise beeinträchtigt ist. In gleicher Weise könnte auch mit einer in der Einheit 1 enthaltenen und von der Ummantelung 2 geschützten Datenübertragungseinrichtung, z.B. einer Magnet- und/oder Sendeimpulse empfangenden und/oder abgebenden Kommunikations-Einheit bzw. einer Antenne, ein Datenaustausch mit der Außenwelt vorgenommen werden. Der Mikroprozessor MP exekutiert aus dem RAM 12. An die Signalaufgabestellen P kann bei Bedarf ein VSS- oder ein VCC-Pegel angelegt werden, somit kann auch die Signalintensität als Meßwert herangezogen werden.

Es ist einfach, die Leitungen 14, die Meßstellen P und/oder Q, Signalgeneratoren und Meßsensoren, Analog/Digitalwandler 5 bzw. Buffer 11 entweder zusätzlich in vorhandene elektronische Recheneinheiten zu integrieren oder mittels bereits in der elektronischen Einheit 1 vorhandenen Leitungen bzw. Schaltbauteilen zu realisieren. In dem üblicherweise vorhandenen Speicher 12, der an den Mikroprozessor MP angeschlossen ist, kann die Signatur gespeichert werden bzw. Signaturvergleiche können dort erfolgen bzw. erfolgt die Speicherung der initial aufgegebenen Daten und/oder Programme.

In Fig. 3 ist der Angriff gegen eine geschützte elektronische Einheit, im vorliegenden Fall ein Mikroprozessor MP, so wie er in Fig. 2 in Draufsicht dargestellt ist, mittels einer Nadel 7 dargestellt. In dem Augenblick, in dem die Nadel 7 die Ummantelung 2 durchdringt, bewirkt die Verletzung der Ummantelung 2 eine unwiderrufliche Veränderung der Signatur. Angedeutet sind ferner eine Signalaufgabestelle P und eine Meßstelle Q, die mit entsprechenden Leiterbahnen 14 an den Mikroprozessor MP angeschlossen sind.

Zur Ermittlung einer Signatur könnte z.B. vorgesehen sein, daß gleichzeitig oder der Reihe nach an fünf Signalaufgabestellen P die Spannungswerte von z.B. +3,+1,+4,0,+1/2 Volt angelegt werden und an einer Anzahl von Meßstellen Q die dort auftretenden Spannungs- und/oder Stromwerte bzw. deren Verläufe und/oder deren Werte gegebenenfalls nach einer bestimmten Zeitspanne als Meßwerte abgenommen werden. Die Meßwerte werden sodann allenfalls nach einer vorgegebenen mathematischen Umformung zur Ausbildung einer Signatur bzw. Zahl herangezogen. Prinzipiell ist es auch möglich, durch entsprechende Ausbildung der Signalgeneratoren und Signalaufgabestellen P und Meßsensoren bzw. Meßstellen Q kapazitive Signale bzw. elektrische Felder als Signale einzusetzen bzw. als Meßgröße zu messen.

Soferne eine elektronische Einheit von einer Ummantelung 2 auf mehreren Seiten umhüllt wird, ist es vorteilhaft, Meßpunkte Q und/oder Signalaufgabepunkte P an jeder dieser Flächen vorzusehen. Eine typische Anzahl von Meßpunkten Q und Signalaufgabestellen P ist zumindest jeweils 20 bis 40 Signalaufgabestellen und Meßpunkte pro cm^2 der Ummantelung 2. Die Anzahl der Meßstellen Q und Signalaufgabestellen P hängt auch von der Größe und Art der Signale bzw. von dem Material der Ummantelung 2 ab. Aus Fig. 1 ist ersichtlich, daß an die Signalaufgabestellen P und an die Meßstellen Q elektrische Leiter 8 angeschlossen sind, welche in verschiedener Länge und/oder verschiedener Dicke und/oder verschiedener Lage in die Ummantelung 2 hineinreichen. Damit kann die Inhomogenität der Ummantelung 2 hervorgerufen bzw. verstärkt und die Signalaufgabe bzw. die Messung der resultierenden Meßgrößen erleichtert werden. Die Form der zu schützenden elektronischen Einheit 1 ist eher nicht relevant, da Ummantelungen 2 aus Kunststoff oder nahezu vergleichbaren Materialien auf alle beliebig gestalteten Oberflächen bzw. um Gegenstände herum aufgebracht werden können.

Des weiteren ist zu bemerken, daß es in der Praxis nahezu unmöglich ist, auch auf zwei gleiche Einheiten 1 idente Ummantelungen 2 aufzubringen, da bereits aufgrund von Herstellungsunregelmäßigkeiten, Oberflächenungenauigkeiten usw., die auf an sich gleich gestaltete Einheiten 1 aufgebrachten Ummantelungen 2 bereits unterschiedliche Eigenschaften besitzen, die für die Ermittlung einer für die Ummantelung charakteristischen Signatur in ausreichender Zahl unterschiedliche Meßwerte zur Verfügung stellen. Es würde auch ausreichen, bei identischen Ummantelungen die Lage der Signalaufgabestellen P und der Meßstellen Q von zwei Einheiten 1 zu variieren, um für diese Einheiten charakteristische und unterschiedliche Signaturen zu erhalten. In die Signatur der Ummantelung 2 gehen ferner nicht nur die Eigenschaften der Ummantelung 2 ein, sondern auch (Oberflächen)Eigenschaften der zu schützenden Einheit 1 ein, insbesondere dann, wenn die Einheit 1 flächig mit der Schutzschicht bzw. Ummantelung 2 in Verbindung steht. Allenfalls wird deshalb zwischen der Ummantelung 2 und einer Schutzschicht eine Isolierschicht angebracht. An sich könnte bereits eine Berührung bzw. ein Anlegen eines elektrischen oder elektromagnetischen Feldes die Signatur - allerdings reversibel - verändern, soferne nicht für eine ausreichende Abschirmung der Ummantelung 2 gegen derartige Einflüsse vorgesehen ist.

Als Sensoren 23 für die Meßwerte können entsprechende analoge Schaltungen eingesetzt werden, die an Analog/Digitalwandler 5 angeschlossen sind. Es können an sich beliebige Einrichtungen zur Ermittlung der Meßwerte vorgesehen bzw. an den Mikroprozessor bzw. Rechner angeschlossen sein.

Wie in Fig. 6 dargestellt, könnte auch zwischen der zu schützenden Einheit 1 und der Ummantelung 2 ein entsprechender Freiraum 16 ausgebildet werden, in dem zu schützende Gegenstände 15 angeordnet werden können. Die elektronische Einheit 1 und der Gegenstand 15 sind allseitig durch eine obere Ummantelung 2' und eine Basis-Ummantelung 2" gegen Zugriff geschützt und zumindest an einer der beiden Ummantelungen 2' sind Signalaufgabepunkte P und Meßstellen Q ausgebildet. Mit einer Zwischenwand 21 könnten die Einheit 1 und der Gegenstand 15 getrennt angeordnet werden. An sich wäre es auch möglich, z. B. die Basis-Ummantelung 2" aus Stahl oder anderem Widerstand gegen Zutritt leistendem Material auszubilden und darauf die von der Einheit 1 überwachte Ummantelung 2' als Schutz gegen unerlaubten Zutritt aufzubringen. Soferne die Basis-Ummantelung 2" bei einem Zugriff zum Gegenstand beschädigt wird, ist dies sichtbar; soferne die elektronisch geschützte obere Ummantelung 2' verletzt wird, bedingt dies eine Fehlfunktion der Einheit 1 aufgrund der veränderten Signatur. Daraus kann festgestellt werden, ob versucht wurde, sich dem schützenden Gegenstand 15 anzunähern. Die in Fig. 6 dargestellte Anordnung kann noch mit einer Umhüllung bzw. Schutzhülle abgedeckt bzw. umschlossen werden.

Fig. 5 zeigt eine Anordnung, bei der auf einem Träger 17 ein Mikrocomputer MC angeordnet ist, dessen strukturellen Aufbau 18 auf einer unteren Trägerschicht 4 ausgebildet wurde und auf dem Leiterbahnen 14 aufgebracht bzw. ausgebildet sind, die durch die Ummantelung 2 nach oben abgedeckt sind. Die Ummantelung 2 kann mit einer Deckschicht 22 abgedeckt werden, die die Signaturwerte der Ummantelung 2 aber eher nicht mitbestimmen soll. Über eine Anschlußleitung 3 steht der zu schützende Mikrocomputer MC mit einer Dateneingabe- und/oder Datenausgabeeinheit 10 in Verbindung, die von der Deckschicht 22 ebenfalls abgedeckt ist. Eine derartige Anordnung kann insbesondere bei einer Scheck- bzw. Bankomatkarte mit Chip- bzw. Mikroprozessor vorgesehen werden. Ein Zugriff von seiten des Trägers 17 durch die Basisschicht 4 des Mikroprozessors MC zerstört diesen unwiderruflich; ein Zutritt durch die Ummantelung 2 zerstört die Signatur und damit ebenfalls die Funktion des Mikroprozessors, sodaß die Einheit unbrauchbar geworden ist.

Es ist möglich, während des Betriebs der elektronischen Einheit, d.h. während der Datenverarbeitung, die Signatur in bestimmten Abständen zu überprüfen und mit einer Weiterverarbeitung der Daten nur dann fortzufahren, wenn die Signatur mit einer gespeicherten vorangehend oder bei der Initialisierung ermittelten Signatur übereinstimmt bzw. als invariant beurteilt worden ist.

Als aufzugebende Signale kommen unter Umständen auch Signalfolgen in Frage, bei denen gleiche oder unterschiedliche Signale bei den Signalaufgabestellen P der Ummantelung aufgegeben werden. Konstruktiv einfach ist es, wenn lediglich eine einzige Signalaufgabeeinheit vorgesehen ist, die an eine Anzahl von Signalaufgabestellen

gleichzeitig oder in einer bestimmten Reihenfolge die Signale aufgibt bzw. nur ein einziger Meßwertaufnehmer vorgesehen ist, der die Meßstellen gleichzeitig oder der Reihe nach abfühlt.

Die Ummantelung 2 kann durchsichtig oder undurchsichtig sein; vorteilhafterweise ist die Ummantelung 2 undurchsichtig, um keine Hinweise auf die präzise Lage der Signalaufgabestellen P und Meßstellen Q zu geben. Über die Ummantelung können beliebige weitere Schichten, Abdeckungen od. dgl. aufgebracht werden.

In Fig. 4 ist beispielsweise ein über den Analog/Digitalwandler 5 an die Einheit 1 bzw. den Rechner angeschlossener Temperatursensor 6 dargestellt, mit dem die jeweilige Temperatur der Ummantelung 2 festgestellt werden kann. Da insbesondere die elektrischen und/oder elektromagnetischen Kennwerte der Ummantelung 2 temperaturabhängig sind, ist die jeweilige Temperatur der Schutzschicht 2 zum Zeitpunkt der Signaturermittlung von Bedeutung. Im Falle unterschiedlicher Temperaturen der zu schützenden Einheit 1 bei der Initialisierung bzw. bei jeweiligen Betriebsbeginnen oder Temperaturänderungen während des Betriebs würden allenfalls unterschiedliche Signaturen ermittelt werden und sich die entsprechenden Folgen einstellen. Es ist somit vorteilhaft, für eine bestimmte Anzahl von Temperaturbereichen jeweils bestimmte unveränderliche Werte der Signatur der Ummantelung 2 im Zuge der Initialisierung zu ermitteln bzw. festzulegen. Die für die einzelnen Temperaturbereiche ermittelten Signaturen S_T, vorteilhafterweise aber nur die Differenzwerte ΔS dieser für die einzelnen Temperaturbereiche ermittelten Signaturen S_T zu einer Norm-Signatur S_{NORM}, die bei einer gewählten Basis- bzw. Normtemperatur ermittelt wurde, werden in der Einheit 1 bei der Initialisierung gespeichert ($\Delta S = S_T - S_{NORM}$). Die bei der Initialisierung im folgenden der Einheit 1 aufgegebenen Daten und/oder Programme werden zumindest teilweise mit der Norm-Signatur S_{NORM} verschlüsselt. Vor oder im Betrieb der Einheit 1 stellt diese die Signatur S_T für die Ummantelung 2 bei der gerade herrschenden Temperatur fest und berechnet aus dieser ermittelten Signatur S_T und dem gespeicherten Differenzwert ΔS für denjenigen Temperaturbereich, in den die herrschende Temperatur der Ummantelung 2 fällt, gemäß obiger Gleichung die Norm-Signatur S_{NORM} mit der die Entschlüsselung der gespeicherten Daten und/oder Programme erfolgt. Ist die Ummantelung 2 beschädigt worden, wird ein unrichtiger Wert für die Signatur S_T ermittelt mit allen Folgen.

Wenn in den Speichern der zu schützenden Einheit lediglich Differenzwerte ΔS der für einzelne Temperaturbereiche ermittelten Signaturen S_T und einer Norm-Signatur S_{NORM}, die z.B. bei 25°C ermittelt wurde, enthalten sind, so wäre sogar das Ausspähen der Differenzwerte ΔS nicht aussagekräftig, da die Norm-Signatur S_{NORM} nicht ermittelt werden kann.

Bei der Ermittlung der Signatur, insbesondere der Signaturen S_T für einzelne Temperaturbereiche, wird vorteilhafterweise derart vorgegangen, daß die ermittelten Signaturwerte bzw. Zahlen gerundet werden, derart, daß die letzte gerundete Stelle innerhalb dieses jeweiligen Temperaturbereiches völlig invariant bleibt. Um den Temperaturgang der Signatur in dem Intervall zu begrenzen werden allerdings so wenig wie möglich Stellen abgeschnitten bzw. werden Zehnerübergänge bzw. die Bit-Sprunggrenzen hauptsächlich durch Veränderung der aufgegebenen Signale im Zuge der Initialisierung ausgeglichen. Ist etwa eine Signatur bzw. Zahl gemäß der Erfindung zu "runden", so wird darauf geachtet, daß bei der Wiederermittlung der Signatur der gleiche Signaturwert entsteht. Man hat daher zu achten, daß kein Meßwert w nach der Rundung aufgrund einer Temperatur- oder Meßtoleranz einmal W und das nächste Mal W+1 ergibt. Demzufolge wird der Meßwert w auf n Stellen abgeschnitten. Liegt der abgeschnittene Wert am Rande des Wertebereiches (besonders nahe der 0 oder des größten möglichen abgeschnittenen Wertes), dann werden andere Signale an die Signalpunkte angelegt, woraus andere Meßwerte resultieren und dies solange bis die letzte Stelle der Signatur für die Grenztemperaturen des Temperaturbereiches gemessen, mit Sicherheit innerhalb dieses Stellenwertes bleibt und diesen Stellenwert nicht nach oben überschreitet.

Bei einer Rundung einer Signatur auf 5 Kommastellen würde die Zahl 34,345325123217218 auf 34,34532 gerundet werden, aber die Zahlen 34,34532001778787 bzw. 34,34532989898567 würden verworfen, weil sie bei einer weiteren Messung eventuell nicht eindeutig identifizierbar bzw. reproduzierbar wären.

Zur Vorgehensweise ist zu bemerken, daß es kein Problem darstellt, die Signalwerte im Sinne der Reproduzierbarkeit im Speicher zu haben, da dadurch keine verwertbare Information über die Meßwerte und damit über die Signatur, die nicht gespeichert werden sollte, resultiert. Die für die Signatur ermittelten Meßwerte können beispielsweise modulo einer Primzahl multipliziert werden.

Für die Initialisierung der elektronischen Einheit 1 wird Sorge getragen, daß diese elektronische Einheit 1 ein Programm besitzt, das eine Signaturermittlung selbständig vornimmt und sämtliche, nach dieser Signaturermittlung für die Initialisierung erhaltene Daten und/oder Programme zum Teil oder zur Gänze mit der ermittelten Signatur verschlüsselt, speichert und abarbeitet. Im Zuge des Betriebs der Einheit 1 von dieser gespeicherte Daten werden mit der jeweils neu ermittelten oder der allenfalls gespeicherten initial ermitttelten Signatur verschlüsselt, gespeichert bzw. abgearbeitet.

Prinzipiell können anstelle von elektrischen und/oder elektromagnetischen Signalen auch Schallsignale, Stoßwellen, Schwingungssignale usw. von der Einheit 1 mit entsprechenden Signalgebern an die Ummantelung 2 angelegt und an den Meßstellen die Meßwerte mit entsprechenden Meßsensoren abgenommen werden, um mit diesen

Meßwerten eine Signatur auszubilden. Die Weiterleitung von Schallwellen, Schwingungen usw. in der Ummantelung 2 hängt direkt von deren Aufbau ab; wird der Aufbau mechanisch verändert, so verändern sich die abgenommenen Meßwerte, da die Signalübertragung in der Ummantelung 2 verändert worden ist.

Es ist vorteilhaft, wenn die bei der Initialisierung ermittelte Signatur nicht gespeichert wird, um ein Ausspähen und damit Entschlüsseln der initial gespeicherten Daten und/oder Programme zu verhindern. Es bringt bereits jedoch Vorteile, wenn die initial ermittelte Signatur gespeichert wird und bei jeder Inbetriebnahme ein Vergleich der initial gespeicherten mit der neu ermittelten Signatur erfolgt; damit kann einerseits der bei Initialisierung der Einrichtung erforderliche Programmieraufwand verringert werden; des weiteren gleichen sich die Signaturen unterschiedlicher Einheiten mit Sicherheit nicht, sodaß auch bei Ausspähen der Signatur einer Einheit keinerlei Rückschlüsse auf die Signaturen von anderen Einheiten gezogen werden können. Von Vorteil ist es, wenn auch bei der Ermittlung der Signaturen für einzelne Temperaturbereiche die Norm-Signatur gemessen bei Normal-Temperatur, nicht gespeichert wird.

Fig. 7 und 8 zeigen Ausführungsformen von erfindungsgemäß ausgebildeten Chipkarten. Fig. 7 zeigt eine Chipkarte 25 mit Kontakten 24 und Fig. 8 zeigt eine kontaktlose Chipkarte 25. Die von einem Chip gebildete elektronische Einheit 1 ist im Fall der Fig. 7 mit Kontakten 24 versehen, die zu einem entsprechenden Datenaustausch mit externen Einheiten dienen. Der Chip 1 selbst ist im wesentlichen bis auf seine Kontaktfläche von einer Ummantelung 2 umgeben, die ihrerseits mit einer Isolationsschicht 26 gegenüber dem Material der Chipkarte 25 isoliert ist. Mit P und Q sind die Signalaufgabestellen und die Meßstellen schematisch dargestellt. Die Verbindung der Kontakte 24 mit dem Chip 1 erfolgt über entsprechende Leiter 3. Das Material der Chipkarte 25 kann an sich beliebig gewählt werden; ein unerwünschter Zutritt zum Chip 1 von seiten der Kontakte 24 her zerstört den Chip 1; ein Zutritt von seiten der Ummantelung 2 zerstört die Signatur unwiderruflich.

Die Ummantelung 2 kann unter Umständen auch mit der Einbettungsmasse 25 ident sein bzw. könnte auch ein Kleber sein, mit dem die Isolierschichte 26 festgehalten wird.

Die in Fig. 8 dargestellte Chipkarte 25 zeigt eine kontaktlose Chipkarte, bei der auch die Antennenspule 10 in die Ummantelung 2 eingeschlossen ist. Es ist durchaus möglich, daß auch die Antenne 10 außerhalb der Ummantelung bzw. der Isolationsschicht 26 in das Material der Chipkarte 25 eingebettet ist. Im vorliegenden Fall ist somit die elektronische Einheit bzw. der Chip 1 allseitig von der Ummantelung 2 geschützt.

Die wesentlichen Vorteile der erfindungsgemäßen Vorgangsweise sind, daß ein Eindringversuch nicht zu einer Zerstörung der zu schützenden Einheit oder der Ummantelung führt, sondern zur Situation, daß die im Bauteil vorhandene Information nicht mehr entschlüsselbar und daher nicht verwendbar wird. Die Anordnung ist so getroffen, daß

sie sich besonders für Microchips eignet. Die Sicherung erfolgt mit einer nicht von außen reproduzierbaren Signatur, die aus der Unregelmäßigkeit des Abdeckmaterials bzw. der Ummantelung abgeleitet wird. Die Methode ist damit auch für alle nichtflüchtigen Speicher, die schützenswerte Information enthalten, geeignet. Ein Löschen der Information und gesonderte Sensoren in diesem Bereich sind zum Schutz der Information daher nicht notwendig.

Patentansprüche:

1. Verfahren zum Schutz von elektronischen Recheneinheiten, Prozessoren, Prozessorschaltungen, insbesondere Mikroprozessoren, Chips, od. dgl., oder derartige Einheiten enthaltende Gegenstände gegen unerwünschten Zugriff, dadurch gekennzeichnet,
   - daß zumindest die einem, insbesondere mechanischem, Angriff bzw. Ausspähen ausgesetzte Seite bzw. Fläche der zumindest einen Prozessor, z. B. einen Mikroprozessor und/oder Rechner und/oder Chip, umfassenden Einheit (1) mit einer Ummantelung bzw. Schutzschicht (2), vorzugsweise mit schwer identisch nachbildbaren, insbesondere in zumindest einer Dimension inhomogenen, elektrischen und/oder elektromagnetischen Eigenschaften, versehen oder abgedeckt wird,
   - daß von der mit der Ummantelung geschützten Einheit (1), insbesondere elektrische und/oder elektromagnetische, Meßwerte, vorzugsweise Widerstand und/oder Kapazität und/oder Strom und/oder Spannung und/oder magnetische Felder und/oder der zeitliche Verlauf dieser Meßwerte, an zumindest einer, vorzugsweise einer Mehrzahl von, vorzugsweise invariant, festgelegten Meßstelle(n) an und/oder in der Ummantelung ermittelt bzw. gemessen werden, nachdem an zumindest einer, vorzugsweise an einer Mehrzahl von, vorzugsweise invariant, festgelegten Signalaufgabestelle(n) an und/oder in der bzw. die Ummantelung (2) von der Einheit (1) definierte, insbesondere elektrische und/oder elektromagnetische, Signale, vorzugsweise Strom- und/oder Spannungssignale, angelegt bzw. eingeleitet wurden,
   - und daß mit den Meßwerten und gegebenenfalls den Signalwerten und allenfalls mit weiteren von der mechanischen Unversehrtheit der Ummantelung abhängigen Meßwerten eine für eine unversehrte bzw. eine durch ihre mit den angelegten Signalen untersuchten Eigenschaften definierte Ummantelung (2) bzw. eine für die Ummantelung zum Zeitpunkt der Vermessung charakteristische Signatur gebildet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Ermittlung der Signatur im Zuge der Initialisierung der Einheit bzw. des Rechners erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß zumindest ein Teil der der Einheit bei ihrer Initialisierung aufgegebenen Daten und/oder Programme unter Einbindung der bei der Initialisierung ermittelten Signatur verschlüsselt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß vor einer, insbesondere vor jeder Inbetriebnahme, und gegebenenfalls auch während des Betriebes der Einheit von der Einheit selbst eine neuerliche Ermittlung der Signatur der Ummantelung unter Zugrundelegung von insbesondere denselben Bedingungen und Vorgangsweisen wie bei der Initialisierung der Einheit vorgenommen wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die im Zuge der Initialisierung ermittelte Signatur nach Verwendung zur Verschlüsselung zumindest eines Teiles der nachfolgend eingegebenen Daten und/oder Programme verworfen bzw. nicht gespeichert bzw. unwiderruflich gelöscht wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Signalaufgabe, die Meßwertermittlung und die Signaturermittlung reproduzierbar vorgegeben sind.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß bei jeder Inbetriebnahme die Signatur neu ermittelt und diese neu ermittelte Signatur zum Entschlüsseln der in dieser Einheit verschlüsselt gespeicherten Daten und/oder Programme herangezogen wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß zumindest ein, vorzugsweise alle Meßwert(e), in ihrer ermittelten Form bzw. Größe oder in einer mathematisch abgewandelten bzw. veränderten Form, gegebenenfalls nach Einsetzen des(r) Meßwerte(s) als Veränderliche in eine (HASH)Funktion zur Bildung der Signatur bzw. des Zahlenwertes der Signatur herangezogen werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß nur bei Feststellung bzw. Verwendung einer unverändert gebliebenen oder einer nur innerhalb von vorgegebenen Grenzen geänderten Signatur die Einheit den ordnungsgemäßen Betrieb aufnimmt oder in den ordnungsgemäßen Betriebszustand versetzt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß die insbesondere zumindest in einer Dimension inhomogene Ummantelung durch vorzugsweise unvollständiges Vermischen von unterschiedlichen, gegebenenfalls nicht bzw. nicht gut miteinander mischbaren Substanzen, z.B. durch Mischen von Kunstharzen bzw. -stoffen, Glas, Gummi od.dgl. und Metallteilchen, Kohlefasern, Rußpartikel od.dgl., oder durch ungleichmäßiges Auftragen von zumindest einem Beschichtungsmaterial, z. B. Kunststoff, hergestellt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß die Beaufschlagung der Signalaufgabestellen mit Signalen und die Ermittlung der Meßwerte zur initialen Festlegung der Signatur und eine neuerliche Ermittlung oder eine Überprüfung der Invarianz der Signatur, insbesondere vor jeder Inbetriebnahme der Einheit, ausschließlich von der mit der Ummantelung geschützten Einheit selbst vorgenommen wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß die im Zuge einer Inbetriebnahme neuerlich ermittelte Signatur nach Verwendung zum Ver- und/oder Entschlüsseln von gespeicherten und/oder zur Speicherung erhaltenen Daten und/oder Programmen verworfen bzw. nicht gespeichert bzw. unwiderruflich gelöscht wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, daß die Auswahl und Reihenfolge der Beaufschlagung der vorhandenen Signalaufgabestellen und die Auswahl und Reihenfolge der Abtastung der Meßstellen, der Art und Größe der Signale, mit denen die Signalaufgabestellen beaufschlagt werden, und die Art und Weise, in der die Meßwerte ermittelt und zur Signatur geformt werden, immer nach einem in der zu schützenden Einheit durch bei der Initialisierung originär gespeicherte Daten und/oder Programme nach einem unabänderlich festgelegten Modus vorgenommen wird.

14. Verfahren nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß bei der Initialisierung für eine Anzahl von unterschiedlichen, insbesondere aufeinanderfolgenden, Temperaturintervallen der Ummantelung jeweils eine Signatur ermittelt wird.

15. Verfahren nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, daß nach Ermittlung von Signaturen für eine Anzahl von unterschiedlichen, insbesondere aufeinanderfolgenden, Temperaturintervallen der Ummantelung lediglich die Differenzen zwischen den für die einzelnen Temperaturintervalle ermittelten Signaturen und einer bei einer vorgegebenen Normaltemperatur bei der Initialisierung ermittelten Norm-Signatur in der Einheit abgespeichert werden, und daß zumindest ein Teil der der Einheit insbesondere bei der Initialisierung aufgegebenen Daten und/oder Programme mit der Norm-Signatur verschlüsselt werden.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, daß bei einer Inbetriebnahme der Einheit aus den für die einzelnen Temperaturbereiche gespeicherten Signatur-Differenzen der der herrschenden Temperatur der Ummantelung entsprechende Wert der Signatur-Differenz herangezogen und zu diesem Wert der bei der herrschenden Temperatur ermittelte Wert der Signatur addiert und damit die Norm-Signatur bei Normaltemperatur ermittelt wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, daß bei der Überprüfung einer vor Inbetriebnahme neuerlich ermittelten Signatur der Signaturwert desjenigen Temperaturintervalles zu Vergleichszwecken herangezogen wird, in dem die zum Zeitpunkt der Signaturermittlung gemessene Temperatur der Ummantelung liegt oder daß der Wert der Norm-Signatur für die Überprüfung der Unversehrtheit der Ummantelung bzw. für die Entscheidung betreffend die Zulässigkeit der Inbetriebnahme der Einheit und/oder das Abschalten derselben herangezogen wird.

18. Anordnung zum Schutz von elektronischen Einheiten, die zumindest eine Recheneinheit bzw. eine Prozessoreinheit, z.B. einen Mikroprozessor und/oder einen Rechner, insbesondere einen Chip, umfassen, gegen unerwünschten Zugriff, insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet,

- daß zumindest die einem, insbesondere mechanischen, Angriff ausgesetzte Seite bzw. Fläche der Einheit mit einer Ummantelung bzw. Schutzschicht (2), vorzugsweise mit schwer identisch nachbildbaren elektrischen und/oder elektromagnetischen Eigenschaften, zumindest teilweise versehen oder abgedeckt ist,
- daß die Einheit (1) zumindest eine Aufgabeeinrichtung (11) umfaßt, mit der zumindest eine, vorzugsweise eine Mehrzahl von Signalaufgabestellen (P) an bzw. in der Ummantelung (2) mit definierten, elektrischen und/oder elektromagnetischen Signalen, vorzugsweise Strom- und/oder Spannungssignalen, beaufschlagbar ist,
- daß die Einheit (1) zumindest eine Empfangseinrichtung (5) zur Ermittlung bzw. Messung zumindest einer Meßgröße bzw. eines Meßwertes umfaßt, die bzw. der von den aufgegebenen Signalen an zumindest einer, vorzugsweise an einer Mehrzahl von an bzw. in der Ummantelung (2) liegenden Meßstellen (Q) hervorgerufen sind (ist),
- und daß zumindest einer, vorzugsweise alle der ermittelten Meßwerte zur gegebenenfalls mathematischen Ermittlung einer für die Unversehrtheit der Ummantelung (2) charakteristischen, von der Einheit (1) im Zuge ihrer Initialisierung ermittelten Signatur (S) verwendet ist bzw. sind.

19. Anordnung nach Anspruch 18, dadurch gekennzeichnet, daß in der Einheit (1) zumindest ein Teil der im Zuge der Initialisierung aufgegebenen Daten und/oder Programme mit der bei der Initialisierung ermittelten Signatur verschlüsselt in einem Speicher (12) abgespeichert sind.

20. Anordnung nach Anspruch 18 oder 19, dadurch gekennzeichnet, daß die Einheit (1) eine Prüfeinheit zur Überprüfung einer jeweils vor Betriebsbeginn der Einheit (1) ermittelten Signatur bzw. zum Vergleich mit einer bei der Initialisierung ermittelten oder mit einer vor einer vorangehenden Inbetriebnahme ermittelten Signatur vorgesehen ist bzw. die Einheit (1) eine derartige Überprüfung vornimmt.

21. Anordnung nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß die Einheit (1) zur neuerlichen Ermittlung der Signatur vor einer Betriebsaufnahme eingerichtet ist und diese neuerlich ermittelte Signatur zur Entschlüsselung der gespeicherten Daten und/oder Programme heranzieht und/oder mit dieser neu ermittelten Signatur die während des Betriebes erhaltenen Daten und/oder Programme verschlüsselt abspeichert.

22. Anordnung nach einem der Ansprüche 18 bis 21, dadurch gekennzeichnet, daß der elektrische Widerstand der gegebenenfalls bezüglich ihrer elektrischen und/oder elektromagnetischen Eigenschaften inhomogen aufgebauten Ummantelung (2) zwischen dem eines Insolators und dem eines metallischen Leiters liegt.

23. Anordnung nach einem der Ansprüche 18 bis 22, dadurch gekennzeichnet, daß die Ummantelung (2) aus nicht bzw. nicht gut miteinander mischbaren Materialien aufgebaut ist und/oder aus zumindest zwei Materialien mit unterschiedlichen elektrischen und/oder elektromagnetischen Eigenschaften und/oder zumindest in einer Dimension, insbesondere bezüglich ihrer Dicke, inhomogen aufgebaut und/oder aus mehreren Schichten unterschiedlicher Dicke und/oder unterschiedlichen Materialien aufgebaut ist.

24. Anordnung nach einem der Ansprüche 18 bis 23, dadurch gekennzeichnet, daß die Signalaufgabestellen (P) und/oder die Meßstellen (Q) unregelmäßig über die Ummantelung (2), insbesondere über deren Innenseite, verteilt festgelegt sind.

25. Anordnung nach einem der Ansprüche 18 bis 24, dadurch gekennzeichnet, daß die Signal-Aufgabeeinrichtung (11) zumindest eine zumindest eine Strom- und/oder Spannungsquelle mit zumindest einer der festgelegten Signalaufgabestellen (P)

verbindende Verteileinrichtung (19) umfaßt, die von dem in der Einheit (1) enthaltenen Mikroprozessor und/oder Rechner (13) steuerbar bzw. an diesen angeschlossen ist.

26. Anordnung nach einem der Ansprüche 18 bis 25, dadurch gekennzeichnet, daß in jeder Meßstelle (Q) ein Meßsensor angeordnet ist, der gegebenenfalls über einen Analog/Digitalwandler (5) an den in der Einheit (1) enthaltenen Mikroprozessor und/oder Rechner (13) angeschlossen ist.

27. Anordnung nach einem der Ansprüche 18 bis 26, dadurch gekennzeichnet, daß die Einheit (1) zur Ermittlung der Temperatur der Ummantelung (2) einen Temperaturfühler (6) umfaßt, dessen Signalausgang gegebenenfalls über einen Analog/Digitalwandler (5) an den Mikroprozessor und/oder Rechner (13) der Einheit (1) angeschlossen ist.

28. Anordnung nach einem der Ansprüche 18 bis 27, dadurch gekennzeichnet, daß in dem Mikroprozessor und/oder dem Rechner (13) Speicherplatz zur Abspeicherung der initial ermittelten Signatur (S) und/oder für für einzelne Temperaturbereiche ermittelte Signaturwerte (S_T) und/oder für Differenzwerte ($S\Delta T$) zwischen den jeweiligen Signaturwerten (S_T) für einzelne Temperaturbereiche und einer für eine bestimmte Normal-Temperatur der Ummantelung (2) bei der Initialisierung ermittelte Norm-Signatur (S_{NORM}).

29. Anordnung nach Anspruch 28, dadurch gekennzeichnet, daß die Einheit (1) einen Differenzbildner aufweist oder zur Differenzbildung eingerichtet ist, um bei der Initialisierung die Differenzen (ΔS) zwischen einer für eine bestimmte Temperatur der Ummantelung (2) ermittelten Norm-Signatur (S_{NORM}) und den für bestimmte Temperaturintervalle der Ummantelung (2) ermittelten Signaturen (S_T) zu berechnen.

30. Anordnung nach einem der Ansprüche 27 bis 29, dadurch gekennzeichnet, daß die Einheit (1) zur Ermittlung der Norm-Signatur (S_{NORM}) einen Addierer aufweist oder zum Addieren eingerichtet ist, um die einer gemessenen Temperatur der Ummantelung (2) entsprechende gespeicherte Differenz-Signatur (ΔS) und die für die vorherrschende Temperatur ermittelte Signatur (S_T) der Ummantelung (2) zu addieren.

31. Anordnung nach einem der Ansprüche 18 bis 30, dadurch gekennzeichnet, daß die Signalaufgabeeinrichtungen und/oder die Empfangseinrichtung(en) mit den Signalaufgabestellen (P) und den Meßstellen (Q) über Leiterbahnen (14) in direktem Kontakt bzw. in direkter leitender Verbindung stehen.

32. Anordnung nach einem der Ansprüche 18 bis 31, dadurch gekennzeichnet, daß von den Signalaufgabestellen (P) und/oder von den Meßstellen (Q) in die Ummantelung (2) unregelmäßig orientierte und/oder gestaltete Leiterbahnen (8) abgehen.

33. Anordnung nach einem der Ansprüche 18 bis 32, dadurch gekennzeichnet, daß die Ummantelung (2) direkt auf die zu schützende Fläche(n) der Einheit (1) aufgebracht ist oder daß die Ummantelung (2) zumindest Teil der Wand (2') eines zu schützende Gegenstände (15) aufnehmenden Raumes (16) ist, in dem vorteilhafterweise auch die Einheit (1) selbst angeordnet ist.

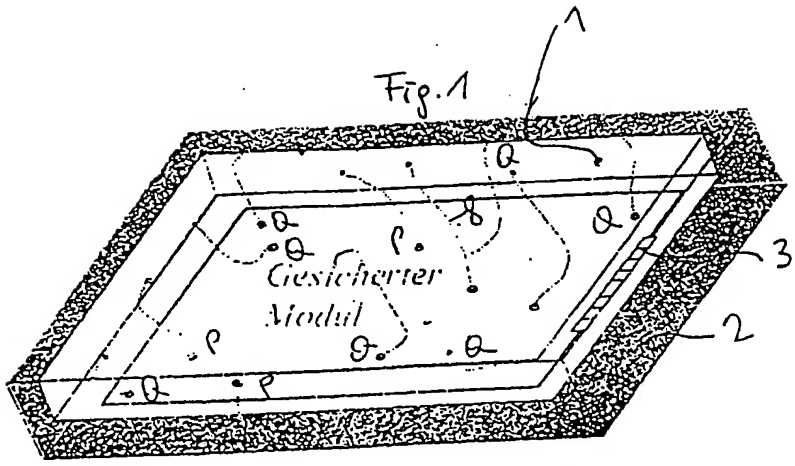
34. Anordnung nach einem der Ansprüche 18 bis 33, dadurch gekennzeichnet, daß zwischen der Ummantelung (2) und der Einheit (1) und/oder zwischen der Ummantelung (2) und einer diese abdeckenden Schicht, z. B. Kunststoffschicht, eine Zwischenschicht, insbesondere elektrische Isolierschicht, angeordnet ist.

35. Anordnung nach einem der Ansprüche 18 bis 34, dadurch gekennzeichnet, daß in keinem Speicher der Einheit (1) die bei der Initialisierung ermittelte Signatur enthalten ist.

36. Anordnung nach einem der Ansprüche 18 bis 35, dadurch gekennzeichnet, daß die Anordnung Teil einer Chipkarte ist.

37. Anordnung nach einem der Ansprüche 18 bis 36, dadurch gekennzeichnet, daß der Chip einer Chipkarte, gegebenenfalls gemeinsam mit Ein- und Ausgabeeinheiten, zumindest auf einer Seite, vorzugsweise allseitig oder auf allen Seiten mit Ausnahme der Kontaktflächen von der Ummantelung (2) umgeben ist, wobei gegebenenfalls zwischen der Ummantelung und dem Kunststoffmaterial der Chipkarte zumindest eine elektrische Isolationsschicht angeordnet ist.

Fig.1



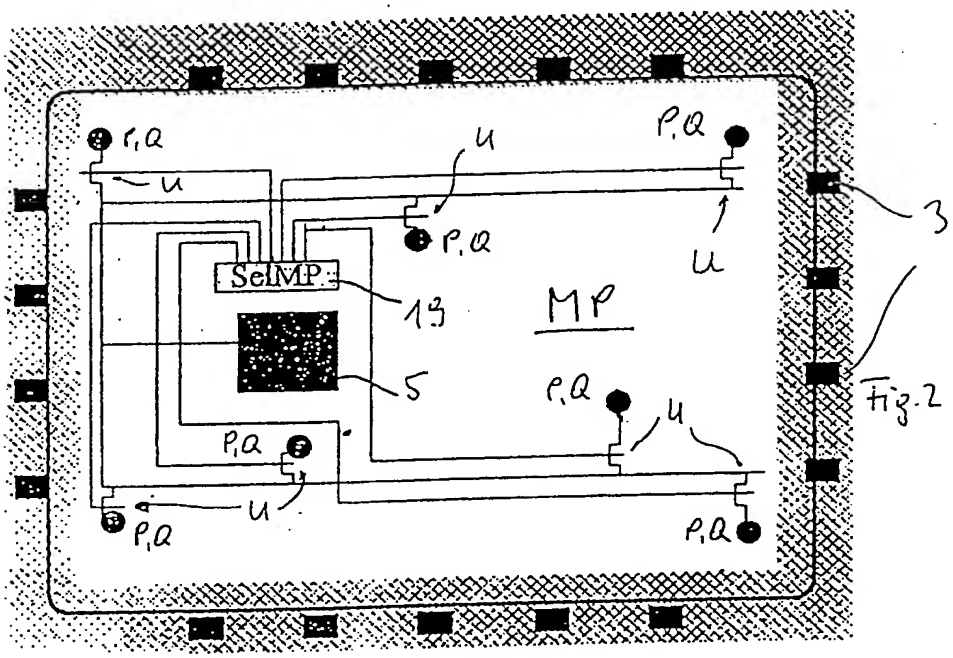


Fig.2

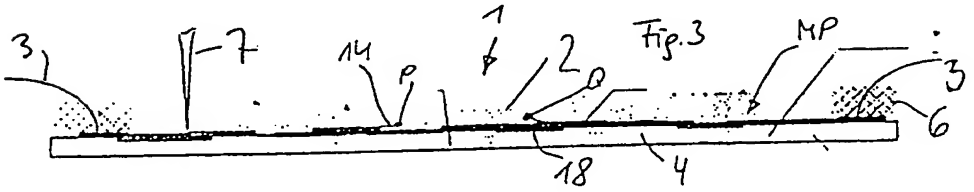


Fig.3

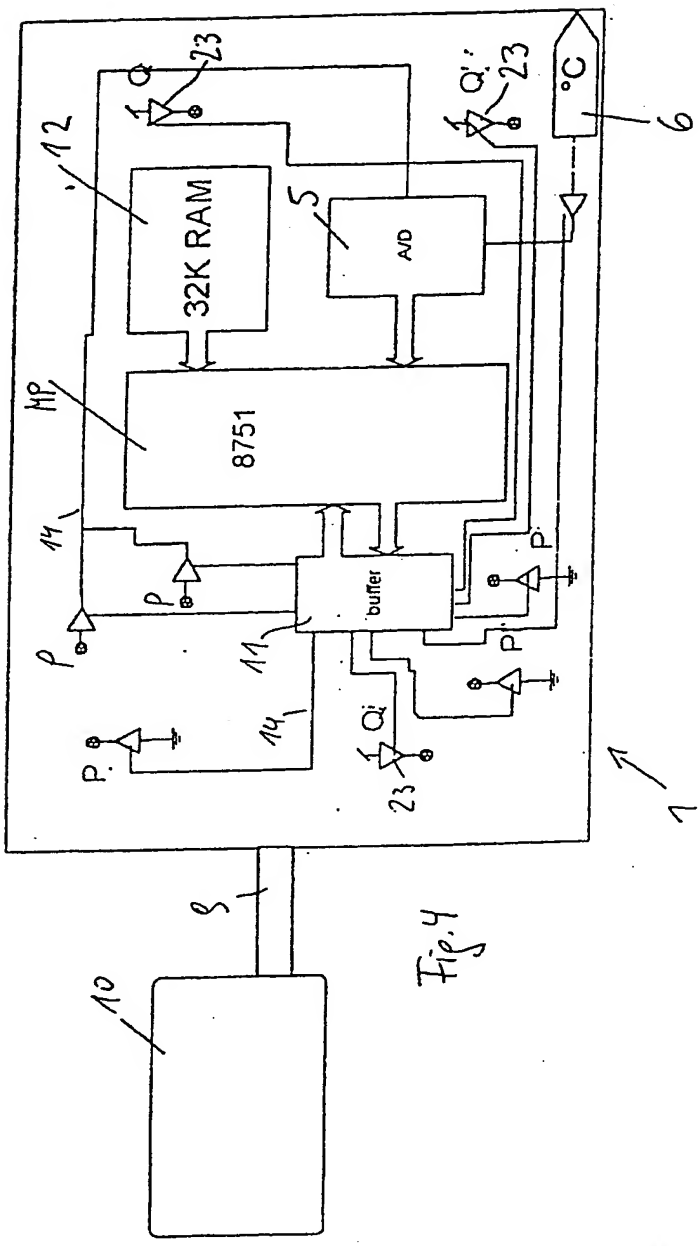


Fig.4

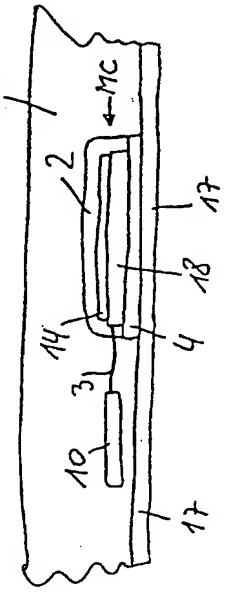


Fig.5

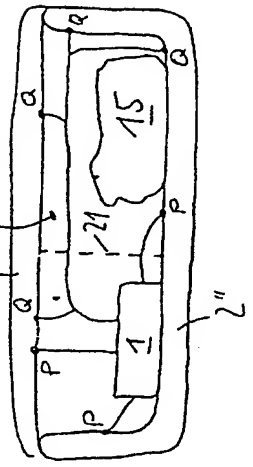


Fig.6

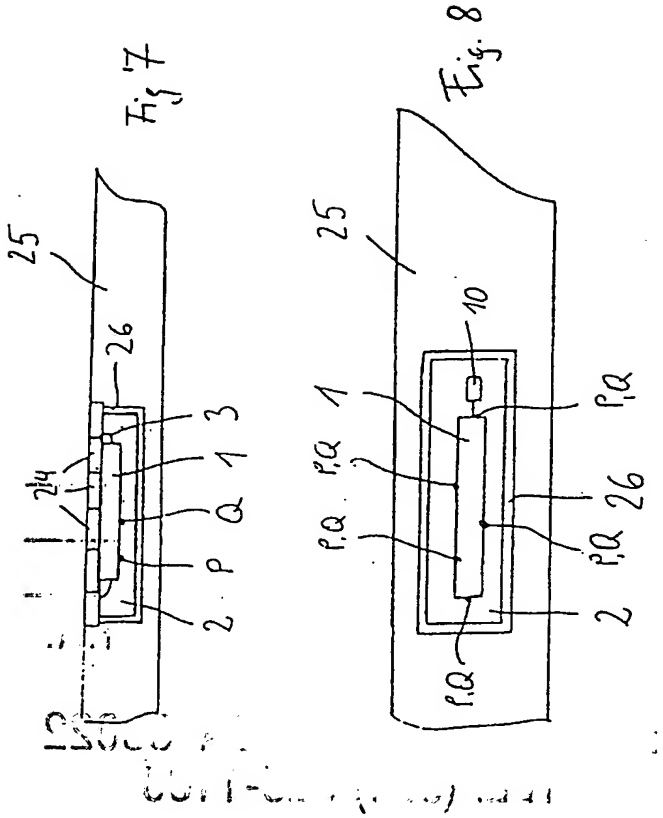


Fig. 7
25
26
2 P Q 1 3
Fig. 8
25
10
P,Q
1
2
26

INTERNATIONAL SEARCH REPORT

International Application No
PCT/AT 97/00225

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 465 349 A (GERONIMI FRANCOIS ET AL) 7 November 1995	1,2,4,6, 9,11,13, 18,20, 25,26, 31,33,36
A	see the whole document	3,5,7,8, 10,12, 14-17, 19, 21-24, 27-30, 32,34, 35,37

DOCKET NO: 1999P1897
SERIAL NO:
APPLICANT: Jorg Schepers
LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 1998	23/01/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Goossens, A

Form PCT/ISA/210 (second sheet) (July 1992)